

EC-Council

Exam Questions 312-50v11

Certified Ethical Hacker Exam (CEH v11)



NEW QUESTION 1

Study the following log extract and identify the attack.

- A. Hexcode Attack
- B. Cross Site Scripting
- C. Multiple Domain Traversal Attack
- D. Unicode Directory Traversal Attack

Answer: D

NEW QUESTION 2

You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command you would use?

- A. `wireshark --fetch "192.168.8"`
- B. `wireshark --capture --local masked 192.168.8.0 ---range 24`
- C. `tshark -net 192.255.255.255 mask 192.168.8.0`
- D. `sudo tshark -f"net 192 .68.8.0/24"`

Answer: D

NEW QUESTION 3

Windows LAN Manager (LM) hashes are known to be weak.
Which of the following are known weaknesses of LM? (Choose three.)

- A. Converts passwords to uppercase.
- B. Hashes are sent in clear text over the network.
- C. Makes use of only 32-bit encryption.
- D. Effective length is 7 characters.

Answer: ABD

NEW QUESTION 4

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The "ps" command shows that the "nc" file is running as process, and the netstat command shows the "nc" process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

- A. File system permissions
- B. Privilege escalation
- C. Directory traversal
- D. Brute force login

Answer: A

NEW QUESTION 5

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

- A. http-methods
- B. http enum
- C. http-headers
- D. http-git

Answer: A

NEW QUESTION 6

Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It doesn't depend on the patches that have been applied to fix existing security holes
- D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

NEW QUESTION 7

John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

- A. Create an incident checklist.
- B. Select someone else to check the procedures.
- C. Increase his technical skills.
- D. Read the incident manual every time it occurs.

Answer: C

NEW QUESTION 8

Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.

After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons. Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?

- A. Warning to those who write password on a post it note and put it on his/her desk
- B. Developing a strict information security policy
- C. Information security awareness training
- D. Conducting a one to one discussion with the other employees about the importance of information security

Answer: A

NEW QUESTION 9

One of your team members has asked you to analyze the following SOA record. What is the version? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

- A. 200303028
- B. 3600
- C. 604800
- D. 2400
- E. 60
- F. 4800

Answer: A

NEW QUESTION 10

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The network devices are not all synchronized.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The attacker altered or erased events from the logs.
- D. The security breach was a false positive.

Answer: A

NEW QUESTION 10

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.

No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

- A. ARP spoofing
- B. SQL injection
- C. DNS poisoning
- D. Routing table injection

Answer: C

NEW QUESTION 13

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?

- A. nslookup -fullrecursive update.antivirus.com
- B. dnsnooping -rt update.antivirus.com
- C. nslookup -norecursive update.antivirus.com
- D. dns --snoop update.antivirus.com

Answer: C

NEW QUESTION 17

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

- A. All are hacking tools developed by the legion of doom
- B. All are tools that can be used not only by hackers, but also security personnel
- C. All are DDOS tools
- D. All are tools that are only effective against Windows
- E. All are tools that are only effective against Linux

Answer: C

NEW QUESTION 19

What port number is used by LDAP protocol?

- A. 110
- B. 389
- C. 464
- D. 445

Answer: B

NEW QUESTION 24

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

- A. har.txt
- B. SAM file
- C. wwwroot
- D. Repair file

Answer: B

NEW QUESTION 25

Which of the following is assured by the use of a hash?

- A. Authentication
- B. Confidentiality
- C. Availability
- D. Integrity

Answer: D

NEW QUESTION 28

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

- A. Time Keeper
- B. NTP
- C. PPP
- D. OSPP

Answer: B

NEW QUESTION 32

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- A. Black-box
- B. Announced
- C. White-box
- D. Grey-box

Answer: D

NEW QUESTION 33

MX record priority increases as the number increases. (True/False.)

- A. True
- B. False

Answer: B

NEW QUESTION 34

Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Physical security
- C. DMZ
- D. Logical interface

Answer: A

NEW QUESTION 37

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.

Which file does the attacker need to modify?

- A. Boot.ini
- B. Sudoers
- C. Networks
- D. Hosts

Answer: D

NEW QUESTION 39

You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best Nmap command you will use?

- A. nmap -T4 -q 10.10.0.0/24
- B. nmap -T4 -F 10.10.0.0/24
- C. nmap -T4 -r 10.10.1.0/24
- D. nmap -T4 -O 10.10.0.0/24

Answer: B

NEW QUESTION 43

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

- A. Trojan
- B. RootKit
- C. DoS tool
- D. Scanner
- E. Backdoor

Answer: B

NEW QUESTION 48

What is a “Collision attack” in cryptography?

- A. Collision attacks try to get the public key
- B. Collision attacks try to break the hash into three parts to get the plaintext value
- C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
- D. Collision attacks try to find two inputs producing the same hash

Answer: D

NEW QUESTION 50

What tool can crack Windows SMB passwords simply by listening to network traffic?

- A. This is not possible
- B. Netbus
- C. NTFSDOS
- D. L0phtcrack

Answer: D

NEW QUESTION 54

One of your team members has asked you to analyze the following SOA record.

What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

- A. 200303028
- B. 3600
- C. 604800
- D. 2400
- E. 60
- F. 4800

Answer: D

NEW QUESTION 56

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

- A. There is no way to tell because a hash cannot be reversed
- B. The right most portion of the hash is always the same
- C. The hash always starts with AB923D
- D. The left most portion of the hash is always the same
- E. A portion of the hash will be all 0's

Answer: B

NEW QUESTION 57

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator’s Computer to update the router configuration. What type of an alert is this?

- A. False negative
- B. True negative
- C. True positive
- D. False positive

Answer: D

NEW QUESTION 59

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Real intelligence
- C. Social intelligence
- D. Human intelligence

Answer: A

NEW QUESTION 64

Which of the following statements about a zone transfer is correct? (Choose three.)

- A. A zone transfer is accomplished with the DNS
- B. A zone transfer is accomplished with the nslookup service
- C. A zone transfer passes all zone information that a DNS server maintains
- D. A zone transfer passes all zone information that a nslookup server maintains
- E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
- F. Zone transfers cannot occur on the Internet

Answer: ACE

NEW QUESTION 66

While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: `nmap -Pn -p- -si kiosk.adobe.com www.riaa.com`. `kiosk.adobe.com` is the host with incremental IP ID sequence. What is the purpose of using "-si" with Nmap?

- A. Conduct stealth scan
- B. Conduct ICMP scan
- C. Conduct IDLE scan
- D. Conduct silent scan

Answer: A

NEW QUESTION 70

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

- A. Use the built-in Windows Update tool
- B. Use a scan tool like Nessus
- C. Check MITRE.org for the latest list of CVE findings
- D. Create a disk image of a clean Windows installation

Answer: B

NEW QUESTION 75

Study the snort rule given below:

From the options below, choose the exploit against which this rule applies.

- A. WebDav
- B. SQL Slammer
- C. MS Blaster
- D. MyDoom

Answer: C

NEW QUESTION 80

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

- A. Clickjacking
- B. Cross-Site Scripting
- C. Cross-Site Request Forgery
- D. Web form input validation

Answer: C

NEW QUESTION 83

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

- A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
- B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
- C. Symmetric encryption allows the server to securely transmit the session keys out-of-band.
- D. Asymmetric cryptography is computationally expensive in comparison.
- E. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

Answer: A

NEW QUESTION 86

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

- A. Application
- B. Transport
- C. Session
- D. Presentation

Answer: D

NEW QUESTION 91

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students. He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- A. Disable unused ports in the switches
- B. Separate students in a different VLAN
- C. Use the 802.1x protocol
- D. Ask students to use the wireless network

Answer: C

NEW QUESTION 95

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

- A. Macro virus
- B. Stealth/Tunneling virus
- C. Cavity virus
- D. Polymorphic virus

Answer: B

NEW QUESTION 97

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms. What is this document called?

- A. Information Audit Policy (IAP)
- B. Information Security Policy (ISP)
- C. Penetration Testing Policy (PTP)
- D. Company Compliance Policy (CCP)

Answer: B

NEW QUESTION 98

Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?

- A. Install DNS logger and track vulnerable packets
- B. Disable DNS timeouts
- C. Install DNS Anti-spoofing
- D. Disable DNS Zone Transfer

Answer: C

NEW QUESTION 101

An LDAP directory can be used to store information similar to a SQL database. LDAP uses a database structure instead of SQL's structure. Because of this, LDAP has difficulty representing many-to-one relationships.

- A. Relational, Hierarchical
- B. Strict, Abstract
- C. Hierarchical, Relational
- D. Simple, Complex

Answer: C

NEW QUESTION 106

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to

implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

- A. Have the network team document the reason why the rule was implemented without prior manager approval.
- B. Monitor all traffic using the firewall rule until a manager can approve it.
- C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
- D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

NEW QUESTION 109

What is the role of test automation in security testing?

- A. It is an option but it tends to be very expensive.
- B. It should be used exclusively
- C. Manual testing is outdated because of low speed and possible test setup inconsistencies.
- D. Test automation is not usable in security due to the complexity of the tests.
- E. It can accelerate benchmark tests and repeat them with a consistent test setu
- F. But it cannot replace manual testing completely.

Answer: D

NEW QUESTION 111

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.

Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

- A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
- B. Bob is partially right
- C. He does not need to separate networks if he can create rules by destination IPs, one by one
- D. Bob is totally wrong
- E. DMZ is always relevant when the company has internet servers and workstations
- F. Bob is partially right
- G. DMZ does not make sense when a stateless firewall is available

Answer: C

NEW QUESTION 115

Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

- A. Preparation phase
- B. Containment phase
- C. Identification phase
- D. Recovery phase

Answer: A

NEW QUESTION 117

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- A. The computer is not using a private IP address.
- B. The gateway is not routing to a public IP address.
- C. The gateway and the computer are not on the same network.
- D. The computer is using an invalid IP address.

Answer: B

NEW QUESTION 120

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.

Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- A. White Hat
- B. Suicide Hacker
- C. Gray Hat
- D. Black Hat

Answer: C

NEW QUESTION 125

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

- A. Randomizing
- B. Bounding
- C. Mutating
- D. Fuzzing

Answer: D

NEW QUESTION 128

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?
alert tcp any any -> 192.168.100.0/24 21 (msg: ""FTP on the network!"");

- A. A firewall IPTable
- B. FTP Server rule
- C. A Router IPTable
- D. An Intrusion Detection System

Answer: D

NEW QUESTION 133

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

- A. list server=192.168.10.2 type=all
- B. is-d abccorp.local
- C. lserver 192.168.10.2-t all
- D. List domain=Abccorp.local type=zone

Answer: B

NEW QUESTION 137

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

- A. Hash value
- B. Private key
- C. Digital signature
- D. Digital certificate

Answer: D

NEW QUESTION 141

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

- A. Wireshark
- B. Ettercap
- C. Aircrack-ng
- D. Tcpdump

Answer: B

NEW QUESTION 142

Which type of security feature stops vehicles from crashing through the doors of a building?

- A. Bollards
- B. Receptionist
- C. Mantrap
- D. Turnstile

Answer: A

NEW QUESTION 146

To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

- A. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
- B. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
- C. If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit
- D. If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Answer: A

NEW QUESTION 149

Identify the correct terminology that defines the above statement.

- A. Vulnerability Scanning
- B. Penetration Testing
- C. Security Policy Implementation
- D. Designing Network Security

Answer: B

NEW QUESTION 151

You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

- A. John the Ripper
- B. SET
- C. CHNTPW
- D. Cain & Abel

Answer: C

NEW QUESTION 154

CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:

From: jim_miller@companyxyz.com

To: michelle_saunders@companyxyz.com Subject: Test message Date: 4/3/2017 14:37

The employee of CompanyXYZ receives your email message.

This proves that CompanyXYZ's email gateway doesn't prevent what?

- A. Email Masquerading
- B. Email Harvesting
- C. Email Phishing
- D. Email Spoofing

Answer: D

NEW QUESTION 156

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

From the above list identify the user account with System Administrator privileges.

- A. John
- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang
- G. Micah

Answer: F

NEW QUESTION 158

Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

- A. SFTP
- B. Ipsec
- C. SSL
- D. FTPS

Answer: B

NEW QUESTION 159

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

- A. Switch then acts as hub by broadcasting packets to all machines on the network
- B. The CAM overflow table will cause the switch to crash causing Denial of Service
- C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF
- D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

Answer: A

NEW QUESTION 164

In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam. Which of the following statement is incorrect related to this attack?

- A. Do not reply to email messages or popup ads asking for personal or financial information
- B. Do not trust telephone numbers in e-mails or popup ads
- C. Review credit card and bank account statements regularly
- D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks
- E. Do not send credit card numbers, and personal or financial information via e-mail

Answer: D

NEW QUESTION 169

What is the algorithm used by LM for Windows2000 SAM?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Answer: B

NEW QUESTION 174

Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

- A. To determine who is the holder of the root account
- B. To perform a DoS
- C. To create needless SPAM
- D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
- E. To test for virus protection

Answer: D

NEW QUESTION 179

You have the SOA presented below in your Zone.

Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

- A. One day
- B. One hour
- C. One week
- D. One month

Answer: C

NEW QUESTION 182

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

- A. Attempts by attackers to access the user and password information stored in the company's SQL database.
- B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
- C. Attempts by attackers to access password stored on the user's computer without the user's knowledge.
- D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Answer: B

NEW QUESTION 185

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

- A. tcp.srcport= = 514 && ip.src= = 192.168.0.99
- B. tcp.srcport= = 514 && ip.src= = 192.168.150
- C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99
- D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

Answer: D

NEW QUESTION 187

Bob received this text message on his mobile phone: "Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com". Which statement below is true?

- A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
- B. This is a scam because Bob does not know Scott.
- C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
- D. This is probably a legitimate message as it comes from a respectable organization.

Answer: A

NEW QUESTION 192

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

- A. Online Attack
- B. Dictionary Attack
- C. Brute Force Attack
- D. Hybrid Attack

Answer: D

NEW QUESTION 196

Which results will be returned with the following Google search query? site:target.com – site:Marketing.target.com accounting

- A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
- B. Results matching all words in the query.
- C. Results for matches on target.com and Marketing.target.com that include the word “accounting”
- D. Results matching “accounting” in domain target.com but not on the site Marketing.target.com

Answer: D

NEW QUESTION 200

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

- A. Traffic is Blocked on UDP Port 53
- B. Traffic is Blocked on TCP Port 80
- C. Traffic is Blocked on TCP Port 54
- D. Traffic is Blocked on UDP Port 80

Answer: A

NEW QUESTION 203

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks
- C. To defend against jailbreaking
- D. To defend against wireless attacks

Answer: B

NEW QUESTION 206

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

- A. USER, NICK
- B. LOGIN, NICK
- C. USER, PASS
- D. LOGIN, USER

Answer: A

NEW QUESTION 210

Fred is the network administrator for his company. Fred is testing an internal switch.

From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

- A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
- B. He can send an IP packet with the SYN bit and the source address of his computer.
- C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
- D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Answer: D

NEW QUESTION 215

In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

- A. Full Blown
- B. Thorough

- Answer: C**

An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

- A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
- B. He will activate OSPF on the spoofed root bridge.
- C. He will repeat this action so that it escalates to a DoS attack.
- D. He will repeat the same attack against all L2 switches of the network.

Answer: A

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers
- E. Have subnet diversity between DNS servers

Answer: BCDE

Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?

```
#include <string.h> int main(){char buffer[8];  
strcpy(buffer, "1111111111111111111111111111");} Output: Segmentation fault
```

- A. C#
B. Python
C. Java
D. C++

Answer: D

Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.

What kind of attack is Susan carrying on?

- A. A sniffing attack
- B. A spoofing attack
- C. A man in the middle attack
- D. A denial of service attack

Answer: C

Which of the following is a low-tech way of gaining unauthorized access to systems?

- A. Social Engineering
- B. Eavesdropping
- C. Scanning
- D. Sniffing

Answer: A

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Answer: B

What is not a PCI compliance recommendation?

- A. Use a firewall between the public network and the payment card data.
- B. Use encryption to protect all transmission of card holder data over any public network.
- C. Rotate employees handling credit card transactions on a yearly basis to different departments.
- D. Limit access to card holder data to as few individuals as possible.

Answer: C

NEW QUESTION 247

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. ESP transport mode
- B. ESP confidential
- C. AH permiscuous
- D. AH Tunnel mode

Answer: A

NEW QUESTION 252

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Answer: B

NEW QUESTION 253

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

- A. 137 and 139
- B. 137 and 443
- C. 139 and 443
- D. 139 and 445

Answer: D

NEW QUESTION 257

An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gain access to the DNS server and redirect the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

- A. MAC Flooding
- B. Smurf Attack
- C. DNS spoofing
- D. ARP Poisoning

Answer: C

NEW QUESTION 258

Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

- A. Honeypots
- B. Firewalls
- C. Network-based intrusion detection system (NIDS)
- D. Host-based intrusion detection system (HIDS)

Answer: C

NEW QUESTION 262

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Traceroute
- B. Hping
- C. TCP ping
- D. Broadcast ping

Answer: B

NEW QUESTION 267

What hacking attack is challenge/response authentication used to prevent?

- A. Replay attacks
- B. Scanning attacks
- C. Session hijacking attacks
- D. Password cracking attacks

Answer: A

NEW QUESTION 270

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

- A. Circuit
- B. Stateful
- C. Application
- D. Packet Filtering

Answer: B

NEW QUESTION 273

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

312-50v11 Practice Exam Features:

- * 312-50v11 Questions and Answers Updated Frequently
- * 312-50v11 Practice Questions Verified by Expert Senior Certified Staff
- * 312-50v11 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-50v11 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-50v11 Practice Test Here](#)